

Kathleen Greenan Ramsey
202.408.6345
kramsey@sonnenschein.com

1301 K Street N.W.
Suite 600, East Tower
Washington, D.C. 20005-3364
202.408.6400
202.408.6399 fax
www.sonnenschein.com

Chicago
Kansas City
Los Angeles
New York
San Francisco
Short Hills, N.J.
St. Louis
Washington, D.C.
West Palm Beach

February 6, 2006

VIA ELECTRONIC DELIVERY

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

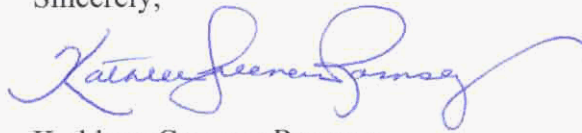
Re: **EB-06-TC-060**
EB Docket No. 06-36
Certification of CPNI Filing February 6, 2006

Dear Secretary Dortch,

Pursuant to the Commission's Public Notice released on January 30, 2006, attached is the proper annual certification of Alltel Corporation, on behalf of its carrier subsidiaries, in compliance with section 64.2009(e) of the Commission's rules, 47 C.F.R. §64.2009(e).

If you have any questions, please do not hesitate to contact the undersigned.

Sincerely,

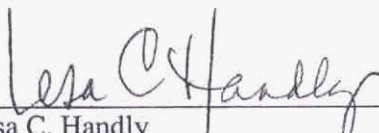


Kathleen Greenan Ramsey
Counsel for Alltel Corporation

cc: Byron McCoy, FCC (*via email* to byron.mccoy@fcc.gov)
Best Copy and Printing, Inc. (*via email* to fcc@bcpweb.com)
Lesa C. Handly, Alltel
Glenn S. Rabin, Alltel

ALLTEL CORPORATION
ANNUAL SECTION 64.2009(e) CERTIFICATION

I, Lesa C. Handly, a duly authorized officer of Alltel Corporation, hereby certify on behalf of Alltel Corporation's carrier subsidiaries,¹ that I have personal knowledge that the Company has operating procedures, as described in the attached PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION, that, to the best of my knowledge, information and belief, are adequate, except as otherwise stated therein, to ensure compliance with the rules of the Federal Communications Commission, codified at 47 C.F.R. Subpart U, implementing Section 222 of the Communications Act of 1934, as amended.



Lesa C. Handly
Senior Vice President - Customer Strategy
Alltel Corporation
February 6, 2006

¹ This certification encompasses Alltel affiliates and subsidiaries during the period of ownership.

STATEMENT REGARDING OPERATING PROCEDURES

The following statement explains how the operating procedures of Alltel Corporation's carrier subsidiaries ensure that it is in compliance with the Commission's CPNI rules, as codified at 47 C.F.R. Subpart U.

Alltel takes seriously its commitment to protect the confidential information of its customers. In addition to internal procedures and protocols to ensure the proper use of customer information, Alltel has numerous security measures in place to protect customer information.

I. PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION

A. Alltel uses CPNI internally for the purpose of providing a customer with the requested service and for marketing service offerings within the categories of service to which the customer already subscribes from Alltel. Alltel presently offers local exchange, CMRS and interexchange service and information services.

B. Alltel does not use, disclose, or permit access to CPNI to market telecommunication service offerings outside the category of service to which the customer subscribes. Segregated databases of CPNI are kept for each service offering.

C. Alltel Communications, Inc. and its CMRS subsidiaries ("ACI") use CPNI derived from the provision of its CMRS services for the provision of CPE and information service(s). Alltel Corporation's LEC and wireline subsidiaries ("Alltel LECs") use CPNI derived from their provision of local exchange service or interexchange service for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

D. Alltel does not permit the use of CPNI to identify or track customers that call competing service providers. For example, Alltel LECs does not use local service CPNI to track customers that call local service competitors.

E. Alltel may also use CPNI internally for the actions identified below;

- (1) to bill and collect for services rendered;
- (2) to provision inside wiring installation, maintenance, and repair services;
- (3) to conduct research on the health effects of CMRS;
- (4) to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking,

call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain Centrex features;

- (5) to protect the rights or property of Alltel, or to protect its users and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, Alltel's services; and
- (6) to provide call location information concerning the user of a commercial mobile service as permitted for E-911 purposes.

F. CPNI may be used only for the purposes identified in Sections A through E above.

G. Alltel has modified both wireless and wireline billing systems to allow for the tracking of a customer's CPNI status.

H. Alltel employees are trained to keep ALL customer data strictly confidential and breaches of customer confidentiality are investigated by corporate security teams. Confirmed unauthorized disclosures of customer data are subject to discipline, including termination and referrals to law enforcement authorities where deemed appropriate. Moreover, customer data for each service offering is partitioned into separate data stores within Alltel's databases.

I. Alltel reviews every sales and marketing campaign that uses customer proprietary data. All such campaigns are conducted within the total service approach. Alltel does not engage in cross service marketing campaigns.

J. Alltel does not sell customer service data.

K. Alltel has established a supervisory review process regarding compliance with its customer privacy and confidentiality procedures for outbound marketing situations. Specifically, each campaign is reviewed by the Director of Campaign Management for compliance with Alltel's privacy and confidentiality procedures. These rules prohibit access to, use, or disclosure of customer private data outside the categories of service to which a customer subscribes.

L. Alltel provides notice in various forms including welcome packages and collateral materials to its customers regarding the customer's right to protect confidential information and the ability to restrict Alltel's use of such information. Alltel has no record of seeking customer opt-out approval in the specific language and format set forth in the Commission rules. The Company is in the process of sending opt-out notices as in the event it is deemed necessary due to the use of independent contractors in marketing efforts within the total service approach. Alltel contracts with independent contractors are required to contain safeguards necessary to protect confidential customer information.

II. ADDITIONAL SAFEGUARDS FOR THE USE OF CUSTOMER INFORMATION

A. Security Governance

Alltel has established an "Enterprise Information Security Program" (EISP) designed to protect all of the data collected, generated, created, stored, managed, transmitted or otherwise handled by the Company. The EISP establishes a Security Steering Committee that includes (among others) the Group President of Operations, the Group President of Shared Services, the General Counsel, the Chief Financial Officer, the Executive Vice President for Network Services and the Senior Vice Presidents of Human Resources and IT Services. The Company has also established a Chief Security Officer responsible for an Enterprise Security Group that develops, implements and enforces security and privacy policies on a Company wide basis.

B. Billing Records, Network Records, and Information

Alltel maintains billing detail data, call detail data, and network record data in applications secured by networks and systems designed to control, monitor, and limit access to authorized users with legitimate business needs.

Internal governance processes dictate that newly created applications and significant changes to existing applications that process or store customer data must be *formally reviewed and analyzed* by appropriate security teams. Alltel's security team reviews each new application or enhancement for compliance with existing security policies, which include requirements for access and authentication controls. Alltel's Internal Audit Department routinely reviews applications to test for compliance with existing security procedures.

C. Data Centers

All data centers have processes and procedures in place for controlling physical access into the data centers along with controlling system access. Compliance with security policies are reviewed by the Enterprise Security team and Internal Audit on a recurring basis.

D. Customer Service Records

Access to customer records is limited to employees based on a need-to-know basis. Initial access to a number of applications is controlled via an internal application that uses role-based logic and employee job requirements, as defined by the designated business owners, to limit access based on job function. Access to all financial reporting relevant applications are reviewed quarterly by the designated business owner for Sarbanes-Oxley compliance.

Alltel has established and communicated its privacy policy through the use of an external information portal. The privacy policy is available at www.alltel.com by clicking on 'Privacy Statement' at the bottom of the home page.

Alltel maintains an account verification policy to ensure that access is only provided to authorized customers, employees and agents. Alltel call center and retail employees are monitored and rated for compliance with Alltel's account verification procedures. These employees are monitored and rated in a number of areas including proper application of the account verification process.